AMENDMENTS TO THE CLAIMS:

The following claims will replace all prior versions of the claims in this application (in the unlikely event that no claims follow herein, the previously pending claims will remain):

1. (**Currently Amended**) An apparatus for providing a trusted channel among secure operating systems (OSs) to which a mandatory access control (MAC) policy is applied, the apparatus comprising:

a data transmission side comprising:

a MAC module for providing MAC information of a user;

a kernel memory for specifying host addresses to which the trusted channel is to be applied and providing an encryption key for encryption of a packet and an authentication key for generation of authentication data; and

a trusted channel sub system that determines, based upon MAC information from the MAC module and the host addresses to which a trusted channel is to be applied from the kernel memory, whether to apply the trusted channel to user data to be transmitted to IP layer; creating a trusted channel header; encrypting a specific portion of the packet; storing the authentication data in the trusted channel header; and transmitting the packet through a network without user manipulation based upon a MAC security class; and

a data reception side comprising:

a trusted channel sub system configured to determine whether the trusted channel is applied; to retrieve the authentication data in the trusted channel header; to decrypt the packet if the authentication data is valid; to conduct trusted channel header processings; and to transfer the packet to an upper level by following a routine for delivering the packet to an input processing section of the upper level to thereby provide the packet to a user on the data reception side; and

a kernel memory configured to provide an authentication key to authenticate the packet and an encryption key to decrypt the packet;

wherein the trusted channel header comprises authentication data to guarantee an integrity of the encrypted data, an initial vector for the decryption of the encrypted data, a next protocol field for a correct upper protocol processing, a header length for identifying a length of

the header, a padding length for indicating a length of padding used for data encryption; and a MAC security class and a MAC category for delivering the MAC information of the user; and

wherein the trusted header is applied without user manipulation if a destination node is a secure OS to which the MAC is applied, and the user has a security class.

2. (Previously Presented) The apparatus of claim 1, wherein the trusted channel is applied when both of following requirements are satisfied: a destination address of the packet corresponds to one of the host addresses to which the trusted channel is applied and the user has a MAC security class; and

wherein the application of the trusted channel is indicated in a next protocol field of an IP header of the packet.

3. (Previously Presented) The apparatus of claim 2, wherein on the data reception side, the application of the trusted channel is determined by checking whether the next protocol field represents the trusted channel header.

4. (Canceled).

5. (Previously Presented) The apparatus of claim 1, wherein the packet, except for an IP header, the authentication data, and the initial vector is encrypted.

6. (**Currently Amended**) A method for providing a trusted channel among secure operating systems (OSs) including a trusted channel sub system and a kernel memory on each of a data transmission side and a data reception side and a MAC module on the data transmission side, the method comprising the steps of:

(a) applying a trusted channel to a user provided packet to be transmitted to the IP layer, based upon the execution of a packet output routine of an Internet Protocol (IP) layer that searches the MAC module and the kernel memory on the data transmission side;

(b) creating a trusted channel header for storing a MAC security class and a MAC category of the user if the trusted channel is applied in step (a);

(c) encrypting all areas of the trusted channel header excluding authentication data and an initial vector; generating authentication information for validating the packet; and storing the authentication information in the trusted channel header;

(d) checksum processing and a fragmentation processing of the packet and providing the packet to the trusted channel sub system on the data reception side through a network by following a lower level output routine;

(e) reassembling and checksum processing, at a reception side IP input processing unit, the packet received at the trusted channel sub system on the data reception side through the network and determining whether the trusted channel is applied to the packet by examining a next protocol field of an IP header in order to decrypt the packet;

(f) retrieving the authentication data in the trusted channel header before decrypting the packet if it is found in the step (e) that the trusted channel is applied to the packet and decrypting the packet if the authentication data is valid while discarding the packet if the authentication data is not valid; and

(g) transferring the decrypted packet to an upper level by following a routine for delivering the packet to an input processing section of an upper level to thereby provide the packet to a user on the data reception side;

wherein the trusted channel header includes a 128-bit authentication data field containing the authentication information for the encrypted packet, a 64-bit initial vector field used as encryption synchronization data of an encryption algorithm, a 8-bit next header field identifying an upper level protocol of IP, a 4-bit trusted channel header length field indicating a length in bytes of the trusted channel header, a 4-bit padding length field designating a length in bytes of a padding used for the encryption of the packet, and a 16-bit MAC security class field and a 64-bit MAC category field showing MAC information of the user who requests the communication; and

wherein the trusted channel is applied without user manipulation ~~based upon the MAC security class~~if a destination node is a secure OS to which the MAC is applied, and the user has a security class.

7. (Previously Presented) The method of claim 6, wherein the applying of the trusted channel in step (a) is determined by examining whether a destination address of the packet corresponds to one of the host addresses to which the trusted channel is applied and whether the user has a MAC security class.

8. (Previously Presented) The method of claim 6, wherein the trusted channel header is recorded in the next protocol field of an IP header of the packet to inform the user on the data reception side that the trusted channel is applied to the packet.

9. (Canceled).